

SYSTEM AND METHOD FOR SECURE STORAGE, TRANSFER AND RETRIEVAL OF CONTENT ADDRESSABLE INFORMATION

ABSTRACT OF THE DISCLOSURE

An algorithm (such as the MD5 hash function) is applied to a file to produce an intrinsic unique identifier (IUI) for the file (or message digest). The file is encrypted using its IUI as the key for the encryption algorithm. An algorithm is then applied to the encrypted file to produce an IUI for the encrypted file. The encrypted file is safely stored or transferred within a network and is uniquely identifiable by its IUI. The encrypted file is decrypted using the IUI of the plaintext file as the key. The IUI serves as both a key to decrypt the file and also as verification that the integrity of the plaintext file has not been compromised. IUIs for any number of such encrypted files may be assembled into a descriptor file that includes meta data for each file, the IUI of the plaintext file and the IUI of the encrypted file. An algorithm is applied to the descriptor file to produce an IUI for the descriptor file. The plaintext descriptor file is then encrypted using the descriptor file IUI as a key for the encryption algorithm. An algorithm is applied to the encrypted descriptor file to produce an IUI for the encrypted descriptor file. The IUI of the encrypted descriptor file is a location-independent identifier to locate the encrypted descriptor file. A flattened descriptor file includes the IUIs of encrypted data files and the IUI of the encrypted descriptor file. An algorithm is applied to the flattened descriptor file to produce its own IUI.